98 P 1607

REF AO

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) Offenlegungsschrift

(10) DE 196 31 360 A 1

B1

(51) Int. Cl.[6]:
H 04 N 7/173
H 04 M 11/00
H 04 M 1/00
H 04 L 9/30
H 04 H 1/00
H 04 B 3/54

(21) Aktenzeichen: 196 31 360.0
(22) Anmeldetag: 2. 8. 96
(43) Offenlegungstag: 5. 2. 98

DE 196 31 360 A 1

(71) Anmelder:
Siemens AG, 80333 München, DE

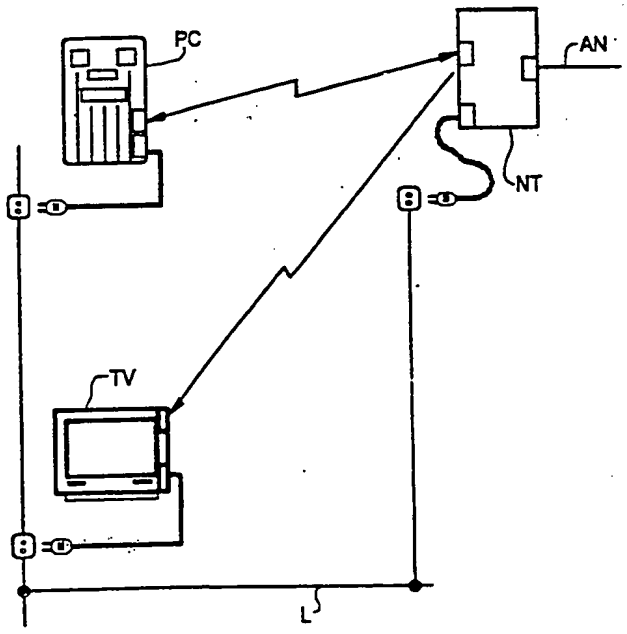
(72) Erfinder:
Möhrmann, Karl-Heinz, Dipl.-Ing., 81369 München, DE

(56) Entgegenhaltungen:
DE 44 08 738 A1
DE 43 42 775 A1
DE 2 96 01 873 U1

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Teilnehmerendgeräte-Anschlußsystem für interaktive Telekommunikationsdienste

(57) Es wird ein Teilnehmerendgeräte-Anschlußsystem mit einer das Teilnehmeranschlußnetz teilnehmerseitig abschließenden Netzabschlußeinheit (NT) und daran angeschlossenen Endgeräten (PC) für interaktive Telekommunikationsdienste beschrieben, das zur Breitbandsignalübertragung zwischen Netzabschlußeinrichtung (NT) und Endgeräten (PC) Breitband-Funkkanäle benutzt und zur Steuerinformationsübertragung zwischen Netzabschlußeinrichtung (NT) und Endgeräten (PC) bidirektionaler Schmalband-Leitungskanal im lokalen Stromversorgungsnetz (Lichtnetz) nutzt.



DE 196 31 360 A 1

Beschreibung

In der modernen Telekommunikationstechnik erwartet die Teilnehmer ein vielfältiges Diensteangebot von konventioneller Telefonie und TV-Signalverteilung bis zu interaktiven Breitband-Telekommunikationsdiensten, deren Signale zu den Teilnehmern hin bzw. von diesen weg über entsprechend ausgebaute Teilnehmer-Anschlußnetze geführt werden (Int. J. of Communication Systems, Vol. 8, 267—274 (1995)). Für diensteintegrierende Netze wird dabei davon ausgegangen, daß das öffentliche Teilnehmer-Anschlußnetz teilnehmerseitig mit einer Netzabschlußeinrichtung (Network Termination NT) abgeschlossen ist; mit dieser Netzabschlußeinrichtung sind dann die (abgesetzten) Teilnehmer-Endgeräte (z. B. Telefon, PC, Set-Top Box mit TV-Empfänger usw.) über entsprechende Leitungen verbunden. Hierfür können gegebenenfalls bereits vorhandene Leitungen verwendet werden; häufig sind aber geeignete Leitungen nicht oder nicht im erforderlichen Umfang vorhanden, so daß eine u. U. aufwendige und kostspielige Neuverlegung von Leitungen im Haus oder Gebäude des Teilnehmers erforderlich wird. Aber auch bei vorhandenem Leitungsnetz ist die Flexibilität begrenzt: Telekommunikations-Endgeräte können nicht an beliebigen Stellen betrieben werden, sondern nur in der Nähe einer geeigneten Anschlußdose. So mag eine HF-Buchse an einer koaxialen Antennenleitung zwar den Anschluß eines TV-Empfängers ermöglichen, ohne daß aber auch ein an einem anderen Aufstellort oder in einem anderen Zimmer betriebener PC an diese Buchse und damit an das koaxiale Hausleitungsnetz angeschlossen werden kann.

Man kann davon ausgehen, daß als nahezu universell verbreitetes Leitungsnetz das 230 V (bzw. 110 V)-Stromversorgungsnetz bei jedem Teilnehmer vorhanden und über die üblichen Steckdosen in allen Räumlichkeiten zugänglich ist, jedenfalls aber dort, wo sich moderne Telekommunikations-Endgeräte befinden, die in der Regel ohnehin einen Anschluß an das Stromversorgungsnetz benötigen. In diesem Zusammenhang ist für interaktive Dienste mit schmalbandigem Rückkanal (wie z. B. Video-Abrufdienste) zur Übertragung der Rückkanalsignale im Teilnehmerbereich die Benutzung des lokalen Lichtnetzes bekannt (DE 43 42 775 A1); alternativ kann man hierfür auch ein schnurloses Telefon verwenden (DE 43 42 776 A1). Eine zusätzliche Übertragung von Datensignalen mit höheren Datenraten, wie sie beispielsweise für "Teleworking" benötigt würden, ist dabei allerdings nicht möglich.

An ein typisches Hausnetz werden sich aber Anforderungen stellen wie beispielsweise:

— bis zu 4 von der Netzabschlußeinrichtung NT zu den Endeinrichtungen führende Abwärtskanäle mit einer Kapazität von jeweils ≤ 4 Mbit/s (4 Mbit/s für Video-Verteildienste bzw. 2 Mbit/s für symmetrische Dienste)

— eine entsprechende Zahl von Aufwärtskanälen mit einer Kapazität von jeweils ≤ 64 kbit/s (für unsymmetrische Dienste wie Videoabruf) oder 2 Mbit/s (für symmetrische Dienste),

und der Erfindung liegt die Aufgabe zugrunde, ein hierfür geeignetes Teilnehmerendgeräte-Anschlußsystem zu schaffen.

Die Erfindung betrifft ein Teilnehmerendgeräte-Anschlußsystem mit einer das Teilnehmeranschlußnetz teilnehmerseitig abschließenden Netzabschlußeinheit [Network Termination NT] und daran angeschlossenen Endgeräten für interaktive Telekommunikationsdienste; dieses Teilnehmerendgeräte-Anschlußsystem ist erfindungsgemäß dadurch gekennzeichnet, daß zur Breitbandsignalübertragung von der Netzabschlußeinrichtung zu einem entsprechenden Endgerät ein Breitband-Funkkanal vorgesehen ist und zur Steuerinformationsübertragung zwischen Netzabschlußeinrichtung und Endgerät ein bidirektionaler Schmalband-Leitungskanal im lokalen Stromversorgungsnetz (Lichtnetz) vorgesehen ist.

Die Erfindung ermöglicht vorteilhafterweise eine einfache, vom Vorhandensein einer geeigneten Verkabelung unabhängige und kostengünstige Realisierung eines Teilnehmerendgeräte-Anschlußsystems zur uni- oder bidirektionalen Übertragung hochratiger Datensignale ohne jegliche Neuverkabelung bei nahezu beliebig hoher Flexibilität bezüglich des Aufstellortes des Endgerätes. Dabei ist auch ein symmetrischer Betrieb (in beiden Übertragungsrichtungen gleich hohe Datenrate) möglich, indem in weiterer Ausgestaltung der Erfindung ein Breitband-Funkkanal auch zur Breitbandsignalübertragung von einem entsprechenden Endgerät zur Netzabschlußeinrichtung hin vorgesehen ist.

Weitere Besonderheiten der Erfindung werden aus der nachfolgenden näheren Erläuterung an Hand der Zeichnung ersichtlich.

In der Zeichnung ist schematisch in einem zum Verständnis der Erfindung erforderlichem Umfang ein Ausführungsbeispiel eines Teilnehmerendgeräte-Anschlußsystems gemäß der Erfindung dargestellt. Dieses Teilnehmerendgeräte-Anschlußsystem weist eine das Teilnehmeranschlußnetz AN teilnehmerseitig abschließende Netzabschlußeinheit (Network Termination) NT und daran angeschlossene Endgeräte für interaktive Telekommunikationsdienste auf. Solche Endgeräte können im einfachsten Fall Telefonapparate sein, ohne daß dies in der Zeichnung näher dargestellt ist. Statt solcher Teilnehmerendgeräte für Schmalband-Telekommunikationsdienste oder auch zusätzlich dazu sind in dem in der Zeichnung skizzierten Teilnehmerendgeräte-Anschlußsystem Endgeräte für unidirektionale oder auch bidirektionale Breitbanddienste vorgesehen, nämlich als Beispiel für einen unidirektionalen Breitbandsignalempfänger ein Videogerät TV und als Beispiel für ein bidirektional mit Breitbandsignalen arbeitendes Gerät ein Personal Computer PC, der über das Teilnehmeranschlußnetz AN mit anderen Computern vernetzt sein möge, ohne daß dies in der Zeichnung näher dargestellt ist.

Zur Breitbandsignalübertragung von der Netzabschlußeinrichtung NT zu einem solchen Endgerät, beispielsweise zum Videogerät TV, ist nun, wie dies auch in der Zeichnung angedeutet ist, ein Breitband-Funkkanal vorgesehen und zur Steuerinformationsübertragung zwischen Netzabschlußeinrichtung NT und Endgerät ein bidirektionaler Schmalband-Leitungskanal im lokalen Stromversorgungsnetz L (häusliches Lichtnetz). In entsprechender Weise ist auch zur Breitbandsignalübertragung von der Netzabschlußeinrichtung NT zu dem bidirektional mit Breitbandsignalen arbeitenden Personal Computer PC ein Breitband-Funkkanal vorgesehen; außerdem ist aber auch, wie dies ebenfalls in der Zeichnung angedeutet ist, ein Breitband-Funkkanal zur Breitbandsignalübertragung vom Personal Computer PC zur Netzabschlußeinrichtung NT hin vorgesehen. Zur Steuerinformationsübertragung zwischen Netzabschlußein-

richtung NT und Personal Computer PC steht wiederum ein bidirektionaler Schmalband-Leitungskanal im lokalen Stromversorgungsnetz L zur Verfügung.

Zum Aufbau einer Breitbandverbindung zwischen Netzabschlußeinrichtung NT und Breitband-Endgerät und zur sicheren und eindeutigen Zuordnung zwischen der Netzabschlußeinrichtung NT und den zugehörigen Endgeräten kann der über das Lichtnetz L geführte bidirektionale Schmalband-Datenkanal genutzt werden, indem ein Endgerät, beispielsweise der Personal Computer PC, über diesen drahtgebundenen Schmalband-Datenkanal an die Netzabschlußeinrichtung NT meldet, daß ein Breitband-Kanal zwischen Netzabschlußeinrichtung und Endgerät aufgebaut werden soll. Der Schmalband-Datenkanal kann dabei der Einfachheit halber im Halb-Duplex betrieben werden, demzufolge abwechselnd jeweils eine Seite sendet, die andere Seite empfängt, und umgekehrt.

Der lichtnetzgebundene bidirektionale Schmalband-Leitungskanal kann ggf. auch als schmalbandiger Aufwärtskanal zur Datenübertragung für unsymmetrische Dienste, z. B. Videoabruf, genutzt werden, ohne daß dies hier noch näher erläutert werden muß.

Um in einem Szenario mit mehreren benachbarten Teilnehmernetzen eine Übertragung der im Schmalband-Datenkanal übertragenen Signale aus dem (z. B. Wohn-)Bereich des Teilnehmers hinaus und damit ein unbefugtes Mithören durch Dritte zu vermeiden, kann zweckmäßigerweise an einer bestimmten Stelle des Hausleitungsnetzes, beispielsweise vor dem Elektrizitätszähler, ein Sperrfilter zur Blockade der Signalübertragung angeordnet sein. Darüberhinaus ist eine noch höhere Datensicherheit dadurch erreichbar, daß die Schmalbandsignale digital übertragen und/oder verschlüsselt werden. Da damit der Kanal für Endgeräte anderer Hausnetze nicht zugänglich ist, ist eine eindeutige Zuordnung zwischen Netzabschlußeinrichtung und Breitband-Endgerät gegeben.

Da ein Funksystem im Prinzip ein Punkt-zu-Multipunkt-System darstellt (ein Sender kann viele Empfänger erreichen), sieht man insbesondere in der Aufwärtsrichtung von den Endgeräten (PC) zur Netzabschlußeinrichtung NT ein geeignetes Vielfach-Zugriffsverfahren vor. Hierbei können Zeitmultiplex- und/oder Frequenzmultiplexprinzipien Anwendung finden. Zweckmäßigerweise sind die Breitband-Funkkanäle indessen CDMA-Kanäle, d. h. es findet hier eine Spread-Spectrum-Technik (auch Code Division Multiple Access CDMA genannt) Anwendung, derzufolge alle Sender dasselbe Frequenzband benutzen, aber die zu übertragenden Bit in Form von unterschiedlichen Folgen aus Nullen und Einsen (sog. Chips) senden. Die unterschiedlichen Chipfolgen werden dabei so gewählt, daß sie möglichst orthogonal zueinander sind, so daß eine zeitrichtige Korrelation eines derartigen empfangenen Basisbandsignals mit derselben Folge ein Ergebnis ungleich Null liefert, während eine Korrelation mit einer anderen (orthogonalen) Folge einen Wert nahe Null ergibt. Spread-Spectrum-Korrelationsempfänger sind an sich bekannt, so daß es hier keiner näheren Erläuterungen dazu bedarf.

Hat ein Breitband-Endgerät bei der Netzabschlußeinrichtung NT einen von dieser zum Endgerät führenden Breitband-Funkkanal angefordert, so "horcht" die Netzabschlußeinrichtung NT zunächst (durch versuchsweise Korrelation mit einer Serie von orthogonalen Chipfolgen, die als digital gespeicherte Tabelle vorliegen), welche Chipfolgen bereits benutzt werden, bis sie eine nicht benutzte Chipfolge findet. Diese Chipfolge verwendet die Netzabschlußeinrichtung NT zum Aufbau des Breitband-Funkkanals (zeitrichtige Multiplikation jedes Bits mit der Folge und anschließende Modulation) und teilt sie über den lichtnetzgebundenen Schmalband-Leitungskanal auch dem betreffenden Endgerät mit, welches seinerseits das empfangene Signal nach Demodulation in das Basisband durch zeitrichtige Korrelation mit dieser Chipfolge decodieren kann.

Wird auch in Aufwärtsrichtung vom Endgerät zur Netzabschlußeinrichtung NT hin ein Breitband-Funkkanal erforderlich, so kann nach der Einrichtung des Abwärts-Funkkanals der hierzu geschilderte Vorgang nochmals mit vertauschten Rollen ablaufen, d. h. das Endgerät sucht eine nicht benutzte Chipfolge, verwendet diese zur Codierung des Upstream-Signals und gibt gleichzeitig die Information über diese Folge über den lichtnetzgebundenen Schmalbandkanal an die Netzabschlußeinrichtung NT. Für eine Mehrzahl von Aufwärtskanälen von mehreren Endgeräten her enthält die Netzabschlußeinrichtung NT eine entsprechende Mehrzahl von Korrelationsempfängern bzw. einen umschaltbaren Korrelationsempfänger.

Das von der Netzabschlußeinrichtung NT abgegebene Breitband-Funksignal kann in einem Szenario mit mehreren eng benachbarten Teilnehmernetzen möglicherweise auch zu Endgeräten gelangen, die eigentlich mit einer ganz anderen Netzabschlußeinrichtungen verbunden sein sollen. Ebenso kann ein Endgerät ein Funksignal abstrahlen, welches von einer anderen als der zugeordneten Netzabschlußeinrichtung aufgefangen und ausgewertet wird. Dies kann ggf. zu Problemen beim Verbindungsaufbau und bei der Sicherheit gegen unbefugtes Mithören und Mißbrauch. Störungen aus benachbarten Netzen werden zwar durch die Wahl jeweils freier Chipfolgen und durch die begrenzte Reichweite (kleine Sendeleistung) mit hoher Sicherheit vermieden. Um aber auch darüber hinaus ein unbefugtes Mithören durch andere Endgeräte aus benachbarten Haus- bzw. Wohnungsnetzen zu unterbinden, kann das digitale Breitbandsignal zusätzlich verschlüsselt werden. Hierzu eignet sich eine generelle Verschlüsselung von Quelle zu Senke oder — systemspezifisch — eine Verschlüsselung unter Verwendung eines sog. Public Key Systems. Dabei wird jeweils aus einem im Endgerät vorgegebenen geheimen Schlüssel ein öffentlicher Schlüssel ermittelt, der über den lichtnetzgebundenen bidirektionalen Schmalband-Leitungskanal in Aufwärtsrichtung zur Netzabschlußeinrichtung NT übermittelt wird, wo er zum Verschlüsseln des für dieses Endgerät bestimmten Funk-Breitbandsignals benutzt wird.

Public-Key-Verfahren sind an sich (z. B. aus ntz 38 (1985) 9, 636, ..., 638) bekannt; sie verwenden zur Schlüsselbildung sog. one-way-Funktionen. Bei one-way-Funktionen handelt es sich um Funktionen, deren Funktionswert relativ einfach zu berechnen ist, während die Berechnung der Inversen kaum möglich ist. "Einfach" und "kaum möglich" meint dabei den rechnerischen Aufwand und hängt somit vom Entwicklungsstand der jeweiligen Computergeneration ab. (Jansen, Pohlmann: "Kryptographie in der Telematik", ntz 38 (1985) 9, 636, ..., 638):

So beruht ein bekanntes Public-Key-Verfahren beispielsweise darauf, daß es ganz einfach ist, durch Multiplikation einer Anzahl von Primzahlen eine große natürliche Zahl zu errechnen, daß es aber kaum möglich ist, diese große natürliche Zahl wieder in ihre Primfaktoren zu zerlegen (Rivest, Shamir, Adleman: "A method for obtaining digital signatures and public-key cryptosy-

stems", Communications of the ACM 21 (1978) 2, 120,..., 126). Bei diesem sog. RSA-Verfahren wird aus einem Klartext M ein Schlüsseltext C durch eine mathematische Tranformation

$$C = M^e \pmod n$$

erhalten. Die inverse Transformation, mit der man aus dem Schlüsseltext wieder den Klartext erhält, lautet

$$M = C^d \pmod n.$$

M ist eine positive ganze Zahl, die zwischen 0 und $n-1$ liegen muß. Es ergeben sich dann die Schlüsselpaare
(e,n) für den öffentlichen Schlüssel und
(d,n) für den geheimen Schlüssel.

Bei der Errechnung der Schlüssel wird zunächst n als Produkt aus zwei sehr großen, frei gewählten Primzahlen p und q berechnet (diese Zahlen werden mittels eines Zufallszahlengenerators erzeugt und bleiben geheim):

$n = p \cdot q$, mit p ungleich q.

Da es zu enormen Schwierigkeiten führt, umgekehrt aus n die Primzahlen p und q zu ermitteln, kann n als Bestandteil des öffentlichen Schlüssels bekanntgegeben werden.

Als geheimer Schlüssel d wird eine große (in ernsthaften Anwendungen ca. 100stellige), frei gewählte ganze Zahl verwendet, die relativ prim zu $(p-1)\cdot(q-1)$ sein muß. Hat man so p, q und d bestimmt, so läßt sich der öffentliche Schlüssel e durch "Inverse Multiplikation":

$$e \cdot d \pmod{(p-1)\cdot(q-1)} = 1$$

erzeugen. Für Primzahlerzeugung und Schlüsselgenerierung existieren spezielle mathematische Algorithmen.

Ein von Zeit zu Zeit vorgenommener Schlüsselwechsel, wie er im Prinzip aus DE 44 35 901 A1 bekannt ist, ist möglich, aber nicht notwendig, was eine Implementierung vereinfacht.

Die vorstehenden, eine Signalverschlüsselung betreffenden Erläuterungen gelten in entsprechender Weise auch für eine Signalverschlüsselung in in Aufwärtsrichtung vom Endgerät zur Netzabschlußeinrichtung NT hin vorgesehenen Breitband-Funkkanälen, ohne daß dies noch weiterer Ausführungen bedarf.

Wollen auch andere Teilnehmerendgeräte Verbindungen mit der selben Netzabschlußeinrichtung NT aufbauen, so geschieht dies in einer den zuvor erläuterten Vorgängen entsprechenden Weise; die Netzabschlußeinrichtung NT moduliert dann aber einen HF-Träger in geeigneter Weise nicht mit nur einem, sondern mit mehreren codierten Signalen.

Das im Vorstehenden erläuterte Teilnehmerendgeräte-Anschlußsystem ist einfach, sicher und kostengünstig zu realisieren, wobei sich beispielsweise folgendes Szenario ergibt:

- bis zu 4 von der Netzabschlußeinrichtung NT zu den Endeinrichtungen führende Abwärtskanäle mit einer Kapazität von jeweils ≤ 4 Mbit/s (4 Mbit/s für Video-Verteildienste bzw. 2 Mbit/s für symmetrische Dienste),
- eine entsprechende Zahl von Aufwärtskanälen mit einer Kapazität von jeweils ≤ 64 kbit/s (für unsymmetrische Dienste wie Videoabruf) oder 2 Mbit/s (für symmetrische Dienste),
- Reichweite ≤ 50 m;

dabei können Fehlverbindungen zwischen benachbarten Haus- bzw. Wohnungsnetzen ausgeschlossen und Sicherheit gegen unbefugtes Mithören oder Emulation eines Teilnehmers gewährleistet werden.

Patentansprüche

1. Teilnehmerendgeräte-Anschlußsystem mit einer das Teilnehmeranschlußnetz (AN) teilnehmerseitig abschließenden Netzabschlußeinheit (NT) und daran angeschlossenen Endgeräten für interaktive Telekommunikationsdienste, **dadurch gekennzeichnet**, daß zur Breitbandsignalübertragung von der Netzabschlußeinrichtung (NT) zu einem entsprechenden Endgerät (PC) ein Breitband-Funkkanal vorgesehen ist und zur Steuerinformationsübertragung zwischen Netzabschlußeinrichtung (NT) und Endgerät (PC) ein bidirektionaler Schmalband-Leitungskanal im lokalen Stromversorgungsnetz (L) vorgesehen ist.
2. Teilnehmerendgeräte-Anschlußsystem nach Anspruch 1, dadurch gekennzeichnet, daß ein Breitband-Funkkanal auch zur Breitbandsignalübertragung von einem entsprechenden Endgerät (PC) zur Netzabschlußeinrichtung (NT) hin vorgesehen ist.
3. Teilnehmerendgeräte-Anschlußsystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Breitband-Funkkanäle CDMA-Kanäle sind.
4. Teilnehmerendgeräte-Anschlußsystem nach Anspruch 3, gekennzeichnet durch eine zusätzliche Verschlüsselung der Breitbandsignale.
5. Teilnehmerendgeräte-Anschlußsystem nach Anspruch 4, gekennzeichnet durch eine Public-Key-Verschlüsselung der Breitbandsignale.
6. Teilnehmerendgeräte-Anschlußsystem nach Anspruch 4 oder 5, gekennzeichnet durch einen von Zeit zu Zeit vorgenommenen Schlüsselwechsel.
7. Teilnehmerendgeräte-Anschlußsystem nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Schmalband-Leitungskanäle Halbduplex-Kanäle sind.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 196 31 360 A1
Int. H 04 N 7/173
Offenlegungstag: 5. Februar 1998